REMARKS

Claim 10 is rejected under 35 U.S.C. 102(b) as being anticipated by White et al. ("White"). Claims 1-6 and 11-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over White in view of Cass. Claims 7-9 and 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over White in view of Cass and further in view of Maher, III et al. ("Maher"). Claims 1 and 10 have been amended. Applicant has also made corrections to the specification, including the Cross-Reference section.

Claims 1 and 10 have been amended to recite steps of creating an anti-virus agent (or "curing" agent). The steps include parsing the virus into three modules, analyzing one of the modules to determine the method of infection, modifying the module to infect client devices already infected by the virus, incorporating the anti-virus into another module that acts to prevent further infection by the virus, and forming an anti-computer virus agent by combining the three modules. These steps are not disclosed, shown, or suggested, in any of the cited references taken alone or in combination.

The invention as recited in the pending claims discloses details of creating an anti-virus agent. In contrast, the *White* reference discusses that an actual virus is forwarded to a central virus analysis center but does not disclose, teach, or suggest, alone or in combination with the other references, the details of how the virus analysis center generates a "cure" for the virus other than the steps of examining a virus signature and other steps, none of which anticipate or render obvious the steps in the presently claimed invention. The focus in *White* is determining that a new virus is present in a network and that a cure can be developed "automatically" without any intervention from humans. Applicant's representative has reviewed the entire *White* reference (not only the cited portions) and has not found any disclosure that teaches or suggests (alone or in combination with Cass) the claimed invention. Steps in claim 1 determine whether a client device has already been infected with a virus (using a detection module). If it has, an anti-virus infection module is "triggered" into the client device to overwrite the virus in the device. Finally, an anti-virus agent payload is used to clean the infected client device and repair any damage done to the device from the virus. This same anti-virus agent payload can also be used to inoculate devices that have not been infected by the virus. Also, the claim recites that the *parsed virus* is *modified* to perform as an anti-virus agent payload. These steps and the steps that

have been added in the present amendment are not disclosed or suggested in the cited references. The *White* reference and the other cited references do not teach creating an anti-virus agent having an infection module that "infects" client devices previously infected with an actual virus, where the new "infection" is the introduction of either an inoculation or remedy, implemented via the payload, tailored to address the specific virus that originally affected the client device.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER LLP

/Rupak Nag/

Rupak Nag
Reg. No. 37,493

P.O. Box 70250
Oakland, CA 94612-0250
Telephone: (612) 252-3335